CYBERARK®

白皮書

CYBERARK 特權存取安全檢疫計畫

www.cyberark.com

目錄

引言

在網路資安計畫中，企業可採取的最有效預防措施之一是保護特權帳號、憑證及秘密資訊。企業紛紛認識到，此過程可能會變得非常複雜，在大企業中尤其如此；然而遺憾的是，保護特權存取不是「一勞永逸」的工作。攻擊者一直不屈不撓尋找企業的安全性漏洞。舉例而言，如果某企業在一年前實施特權存取保護計畫，而現在他們可能有新的基礎架構、新的 SaaS 應用程式或使用 DevOps 方法開發的應用程式、更廣泛的雲端產品組合，還有規劃中的資料中心整合。為了最有效地抵禦攻擊，企業需要確保他們的特權存取安全計畫處於最新狀態，而且需要繼續保護最關鍵的基礎架構、應用程式、客戶資料、智慧財產權及其它重要資產。

Forrester Research 在報告中稱：「企業讓攻擊者得以存取超過 10 億筆客戶記錄」，這還不包括雅虎資料外洩事件中遭洩露的估計大約 5 億筆記錄。[1]

2017 年報告提到「81% 的資料外洩事件中，駭客利用遭竊取的帳密及弱密碼進行攻擊。」[2]

要積極主動地降低攻擊者造成的特權存取風險，企業一般需要：

- 理解以特權存取為攻擊手法的常見攻擊類型：在每種情況下，為了攻擊企業的安全性漏洞，攻擊者是怎麼想、怎麼做的？
- 決定最重要的特權帳號、憑證及秘密資訊的優先順序，找出現有特權存取安全計畫中潛在薄弱環節及安全性漏洞，尤其是有可能危及關鍵基礎架構及企業最重要資產的安全性漏洞。
- 確定「清除」這些薄弱環節及潛在安全性漏洞的最有效措施。何種安全措施應優先處理？哪些可快速實現？哪些需要更長期的計畫？
- 確保持續特權存取檢疫計畫的進行、重新評估及改進，以面對不斷變化的環境威脅。

[1] Balouras、Stephanie 等，《2016 年全世界最重大資料外洩及隱私侵權事件所帶來的經驗教訓》，Forrester Research 公司，2017 年 1 月 9 日 | 更新：2017 年 2 月 15 日，第 2 頁。

[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/#report

CyberArk 特權存取安全網路檢疫計畫概述

CyberArk 發展出一套系統化方法，幫助企業通過建立及維護強大的特權存取安全檢疫計畫來保護自身。CyberArk 特權存取安全檢疫計畫充分利用 CyberArk 資安團隊在處理重大資料外洩事件的過程中所積累的廣泛經驗，包括與許多大企業的合作經驗。通常，這些資安事件的罪魁禍首都是最常見的特權存取攻擊，每個事件為我們都提供與攻擊相關的寶貴資訊，進一步能了解攻擊者如何操作且攻擊企業的安全性漏洞。

透過集中且協作的系統化資安服務，可幫助企業建立基本的特權存取檢疫控制機制來增強總體安全性。有效實施這種類型的計畫，有助於企業在更短的時間內更有效地降低風險，且以更少的內部資源來提升安全性並符合監管的要求。

本安全檢疫計畫的目標是協助企業可制定且順利實現以下目標：對於特權帳號、憑證及秘密資訊的最常見攻擊，可達到最高層級的資安保護。[圖 1]

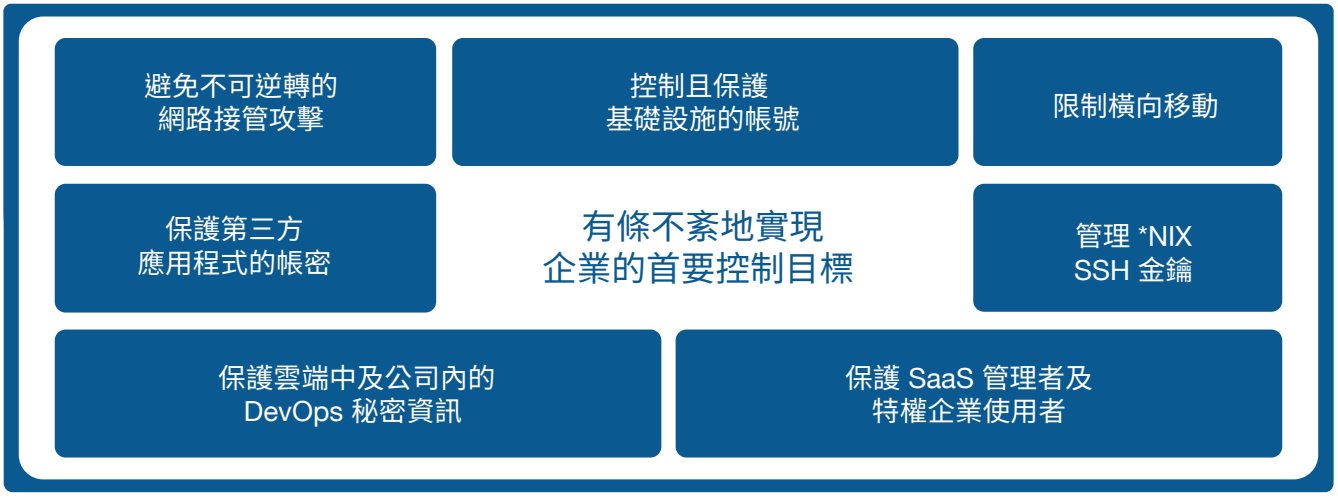

圖 1: CyberArk 特權存取安全網路檢疫計畫的總體目標著重於滿足最重要的需求，對於企業面臨的潛在安全性漏洞，提供對最重要的特權存取的有效保護，例如對關鍵基礎架構及應用程式、客戶資料及企業最重要資產的存取，確實保護在公司內或是在雲端的安全。

達到最有效的特權存取保護

為了實現最有效的保護，CyberArk 資安團隊與企業密切合作以完成：

- 共同分析評估與現有特權存取安全計畫相關的風險，運用對攻擊者思維模式及戰術的瞭解，找出計畫中薄弱的環節。
- 定義所需的保護措施且制定優先順序。
- 建立最佳方法與實施計畫，以達到適當等級的保護。

每家企業的特權存取安全檢疫計畫都是獨一無二的。然而，以下簡要介紹 CyberArk 資安團隊如何應對最常見的特權存取攻擊。某些企業可能需要在每個領域都著墨，但更常見的情況是，某些企業只能保護最關鍵的資產，至少最剛開始是這樣。不管您的應用程式及基礎架構部署在公司內、在雲端中 (IaaS、PaaS 及 Saas) 還是混合環境中，這種方法都適用。

防止不可逆轉的網路接管攻擊

攻擊者的想法

發動難以察覺、破壞性很強、且能迫使企業不得不進行重建 IT 系統以抵禦攻擊者於門外的攻擊【如萬用票證 (Golden Ticket) 等 Kerberos 攻擊】，進而在企業中站穩腳跟。

萬用票證不僅僅是經過篡改的 Kerberos 票證——這是一種經過篡改的 Kerberos 金鑰發佈中心，讓攻擊者可在 Kerberos 身份驗證功能允許的範圍內為所欲為長達數年的時間。

→

在您**當前**的特權存取安全計畫中：

- **貴公司是否依賴單因子身份驗證來驗證網域管理者進行身份？**
- **使用雜湊 (hash) 是否可在第 0 層系統及第 1/2 層中某些機器進行特權存取？**

防止此類攻擊的**最有效保護措施**包括：

- 隔離對第 0 層及第 1 層的所有特權存取，且要求進行多因子身份驗證
- 設計過程中不留下任何雜湊
- 及時發現且攔截對網域控制站 (Domain Controller) 正在進行的 Kerberos 攻擊
- 阻斷在第 0 層新增基礎架構帳號

→

達到最佳保護的**途徑**：

- 只允許通過多因子身份驗證的使用者存取 CyberArk 核心特權存取安全解決方案
- 運用網域控制站保護 (Domain Controller Protection) 產品選項及 CyberArk 終端特權管理器的 CyberArk 核心特權存取安全解決方案來保護網域控制站及其它第 0 層及第 1 層的資產

控制且保護基礎架構帳號

攻擊者的想法

利用強大的預設基礎架構帳號——這些帳號存在於公司內或雲端環境中，在日常維運中很少使用，但可創造攻擊者絕佳的存取機會。例如，攻擊者可利用未修改的預設密碼來破解基礎架構帳號，進而接管整個基礎架構。相同的憑證或帳密可用於存取類似的資產。

→

在您**當前**的特權存取安全計畫中：

- **有多少本地管理者帳號保存在以下伺服器中：**
  - Windows 伺服器？
  - *NIX 伺服器？
  - Cisco 設備？
  - SQL 資料庫伺服器？
- **Oracle 伺服器上的 SYS 及 SYSTEM 情況如何？**
- **貴公司如何保護雲端基礎架構帳號？**

防止此類攻擊的**最有效保護措施**包括：

- 確保所有帳號都受到有效保護

→

達到最佳保護的**途徑**：

- 利用 CyberArk 核心特權存取安全解決方案，將所有眾所周知的基礎架構帳號保存在數位密碼金庫中
  - 定期或在每次使用後自動更替密碼

限制橫向移動

攻擊者的想法

透過在基礎架構內橫向移動來竊取憑證或帳密，例如使用雜湊傳遞 (Pass-the-Hash) 方法，以獲取更大的權限。

→

在您**當前**的特權存取安全計畫中：

- **多少 IT Windows 工作站中的終端使用者有本地管理者權限？**

防止此類攻擊的**最有效保護措施**包括：

- 從 IT Windows 工作站的本地管理者群組中徹底移除所有終端使用者

→

達到最佳保護的**途徑**：

- 利用 CyberArk 終端特權管理器，撤銷 IT Windows 工作站中的本地管理者權限，防止憑證或帳密遭到竊取

保護第三方應用程式的憑證或帳密

攻擊者的想法 入侵用於執行深度掃描等操作的第三方應用系統，以竊取其中內嵌的特權帳密。藉此，攻擊者就可達到攻擊目的，同時完全合法繞過的安全防線。	→	在您**當前**的特權存取安全計畫中： • **有多少已安裝的應用程式及資安解決方案需要使用可全面存取 IT 環境以完成相關操作的高權限帳號？** • **這些特權帳號中有多少保存在數位密碼金庫中？** – 弱點掃描引擎？ – 電腦盤點管理程式及應用程式伺服器？ – WebLogic/WebSphere/Tomcat/JBoss 所儲存的資料庫密碼？
防止此類攻擊的**最有效保護措施**包括： • 將協力廠商應用程式使用的所有特權帳號保存在金庫中	→	達到最佳保護的**途徑**： • 運用 CyberArk 核心特權存取安全解決方案，且設定為在每次使用後自動更替密碼 • 運用 CyberArk 應用程式身份管理器來移除套裝應用程式中寫死的帳密

管理 *NIX SSH 金鑰

攻擊者的想法 利用不受管理的 SSH 金鑰來以 root 存取權限登入且接管 *NIX 技術堆疊。Unix/Linux 系統中儲存企業內部分最敏感的資產。而用於取得 root 特權的個人帳號（包括 SSH 金鑰）通常被資安團隊所忽略。	→	在您**當前**的特權存取安全計畫中： • **Unix 及 Linux 實際執行伺服器中有多少不受管理的 SSH 金鑰對？**
防止此類攻擊的**最有效保護措施**包括： • 將生產環境中 Unix 及 Linux 伺服器內的所有 SSH 金鑰都保存在數位密碼金庫中且定期更替	→	達到最佳保護的**途徑**： • 將生產環境中 Unix 及 Linux 伺服器內的 SSH 金鑰保存在數位密碼金庫中且定期自動進行更替，並運用 CyberArk 核心特權存取安全解決方案，依據資安政策進行保護

保護雲端中及公司內的 DevOps 秘密資訊

攻擊者的想法 獲取原始碼及 CI/CD 工具中所儲存的高權限 API 金鑰，以攻擊環境，獲得更廣泛的存取權限。	→	在您**當前**的特權存取安全計畫中： • **Ansible、Jenkins、Docker 及其它 DevOps 工具中使用的秘密資訊及帳密是否嵌入在任意文字 (free text) 中或採用寫死的方式？** • **您是否使用多種 DevOps 工具，這些工具不共用集中功能來保存秘密資訊，而無法統一管理？您能否稽核哪些應用程式及工具在使用特定秘密資訊？** • **有多少公有雲 / 私有雲 root 帳號及 API Key 沒有保存到數位金庫中且定期進行更替？(如 AWS root 存取及預設 API Key)**
防止此類攻擊的**最有效保護措施**包括： • 將公有雲的特權帳號、金鑰及 API Key 保存在數位金庫中並自動定期更替 • 納管 Ansible、Jenkins 及 Docker 等 CI/CD 工具使用的憑證、帳密及秘密資訊保存在數位金庫中，可快速檢索，且自動更替	→	達到最佳保護的**途徑**： • 使用 CyberArk 核心特權存取安全解決方案管理 root 帳號 金鑰及 API Key 實現安全的儲存及自動定期更換。 • 使用 CyberArk Conjur 來保護、儲存及存取 DevOps 及其它動態環境中的機器身份及使用者所使用的秘密資訊 (如 CI/CD 工具中的內嵌的 Key 或帳密) • 使用 CyberArk 應用程式身份管理器，在更靜態的應用程式環境 (一般部署在公司內) 中保存及管理特權帳密及秘密資訊。

保護 SaaS 管理者及特權企業使用者

攻擊者的想法 竊取 SaaS 管理者及企業高權限使用者所使用的 Key、憑證或帳密，以獲取高階權限，悄悄存取敏感系統。	→	在您**當前**的特權存取安全計畫中： • **有多少 ERP 及財務部門所使用的網站的高權限 ID 在財務部門的同仁間共用？** • **有多少人事系統的高權限 ID 在人力資源部門的同仁間共用？** • **您如何保護可存取社群媒體、銷售運營及財務應用程式等敏感應用程式的 SaaS 管理者？** 附註：由於這些 ID 通常是共用的，因此身份驗證是不使用多因子身份驗證方法
防止此類攻擊的**最有效保護措施**包括： • 隔離對共用 ID 的所有存取，且要求進行多因子身份驗證	→	達到最佳保護的**途徑**： • 只允許通過多因子身份驗證的使用者存取 CyberArk 核心特權存取安全解決方案 • 利用 CyberArk 核心特權存取安全解決方案 (其中包括防篡改稽核日誌、監控及記錄、以及連線隔離功能)，保護對敏感應用程式的所有共用 ID 及 SaaS 管理者的高權限存取

下一步

維護最有效保護的特權存取，需要資安團隊時時刻刻保持警覺。CyberArk 提供多種解決方案及功能，幫助企業持續改進其特權存取安全計畫，增強企業的總體安全性。這包括：

- 衡量進展：CyberArk 探索及稽核（Discovery and Audit，DNA）是一個強大的工具，可用於定期掃描企業的基礎架構，及時發現可能隱藏但不受保護的特權存取，包括雲端及 DevOps 環境。
- 驗證且改進對防禦實際攻擊的有效性。CyberArk Red Team 可在部署前及部署完成後進行攻擊演練，以驗證控制措施的有效性。
- 增強公司內員工的知識水準、專業技術及意識。例如，這包括：
  - CyberArk 培訓及認證服務讓企業可幫助內部團隊成員獲得 CyberArk 認證的能力及專業技術
  - CyberArk 及合作夥伴的資安服務可幫助企業加速計畫實施及知識傳授。

CyberArk 特權存取安全檢疫計畫讓企業可採取系統化方法來改進總體特權存取安全性。攜手 CyberArk 資安團隊，企業應能夠解決與其總體企業資安策略及狀態相關的關鍵問題。此計畫旨在幫助企業在更短的時間內能更大幅度降低風險，順利提升整體安全性及達到監管合規性目標，而不增加企業內部人員的負擔。

若欲更詳細瞭解如何運用 CyberArk 資安服務來保護特權帳號安全，請瀏覽：www.cyberark.com。